CARPATHIAN J. MATH.
0 (0), No. 00 - 00,

Some properties of the symbol algebras

DIANA SAVIN, CRISTINA FLAUT, CAMELIA CIOBANU

ABSTRACT. In this paper, we obtain some properties of the symbol algebras, starting from their connections with the quaternion and cyclic algebras over a field K_p,where K is an algebraic number field, p is a prime in K and K_p is the completion of K with respect to $p-$ adic valuation, in the case when $K = \mathbb{Q}(\varepsilon)$, $\varepsilon^3 = 1, \varepsilon \neq 1$.

1. Introduction

Symbol algebras have many applications in number theory (class field theory), as can be seen in [4], [6], [7]. Since they are a natural generalization of the quaternion algebras, in this paper we find some interesting example of split quaternion algebras and non division symbol algebras and we give a necessary and sufficient condition for a K_v-cyclic central simple algebra $A = \left(\frac{\alpha,\beta}{K,\epsilon}\right)$ to be a division algebra.

First, we recall some definitions in the theory of associative algebras.

Let $A \neq 0$ be an algebra over the field K. If the equations $ax = b$, $ya = b, \forall a, b \in A, a \neq 0$, have unique solutions, then the algebra A is called a *division algebra.* If A is a finite-dimensional algebra, then A is a division algebra if and only if A is without zero divisors ($x \neq 0, y \neq 0 \Rightarrow xy \neq 0$).(see [9])

Let K be a field with $charK \neq 2$. Let $\mathbb{H}_K(\alpha, \beta)$ be a quaternion algebra with basis $\{1, e_1, e_2, e_3\}$ and the multiplication given by

$\cdot$	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	α	e_3	αe_2
e_2	e_2	$-e_3$	β	$-\beta e_1$
e_3	e_3	$-\alpha e_2$	βe_1	$-\alpha\beta$

.

Each element $x \in \mathbb{H}_K(\alpha, \beta)$ has the form $x = x_0 \cdot 1 + x_1 e_2 + x_2 e_2 + x_3 e_3$, with $x_i \in K$, $i = 0, 1, 2, 3$. For $a \in \mathbb{H}_K(\alpha, \beta)$, $a = a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3$, the element $\bar{a} = a_0 - a_1 e_1 - a_2 e_2 - a_3 e_3$ is called the *conjugate* of the element a. Let $a \in \mathbb{H}_K(\alpha, \beta)$. We have that $t(a) \cdot 1 = a + \overline{a} \in K$, $n(a) \cdot 1 = a\overline{a} \in K$ and these are called

[1]For the first author, the research for this article was carried out during her visit at the Central European University (CEU), Budapest, from 1 January to 31 March 2008, and supported by the CEU Special and Extension Program.

Received: 7.11. 2008; In revised form: ; Accepted:

2000 *Mathematics Subject Classification.* 17A35, 11S31.

Key words and phrases. *symbol algebras, p-adic valuation, Artin symbol*

Accepted on June 2, 2009.

the *trace*, respectively, the *norm* of the element $a \in A$. It follows that $(a+\overline{a})\, a = a^2+\overline{a}a$=$a^2+n\,(a)\cdot 1$ and $a^2-t\,(a)\, a+n\,(a)=0, \forall a \in A,$ therefore the generalized quaternion algebras are *quadratic*. We remark that $n\,(a)=a_0^2-\alpha a_1^2-\beta a_2^2+\alpha\beta a_3^2$. The generalized quaternion algebras is a division algebra if and only if for $x \in \mathbb{H}_K\,(\alpha,\beta)$ we have $n\,(x)=0$ only for $x=0$. Otherwise, the algebra $\mathbb{H}_K\,(\alpha,\beta)$ is *a split* algebra.

An important invariant for a quaternion algebra $\mathbb{H}_K\,(\alpha,\beta)$ is the *associated conic*, denoted $C\,(\alpha,\beta)$. The associated conic is the projective plane curve defined by the homogeneous equation $\alpha x^2+\beta y^2=z^2$.

Let K be an algebraic number field. By a prime of K we mean a class of equivalent valuations of K. Recall that the finite primes of K are in one-to-one correspondence with the primes ideals of the ring of integers of K, and the infinite primes are in correspondence with the embedding of K into the field of complex numbers $\mathbb{C}$. If v is a prime of K, we denote with K_v the completion of K with respect to the v-adic valuation.

Proposition 1.1. [4, pag. 7]*The quaternion algebra $\mathbb{H}_K\,(\alpha,\beta)$ is split if and only if the conic $C\,(\alpha,\beta)$ has a rational points over K(i.e. if there are $x_0,y_0,z_0 \in K$ such that $\alpha x_0^2+\beta y_0^2=z_0^2$).*

A natural generalization of the *quaternion algebra* is the *symbol algebra*, also known as a *power norm residue algebra*. J. Milnor, in his book *Introduction to Algebraic K-Theory*, calls it the *symbol algebra* because of its connection with the $K-$theory and with the Steinberg symbols.(see [8])

A *symbol algebra* is a unitary associative algebra over a field K with $\zeta \in K, \zeta^n=1, \zeta$ a primitive root, generated by the elements x,y which satisfy the relations $x^n=\alpha, y^n=\beta$ and $yx=\zeta xy$. This algebra is denoted $\left(\frac{\alpha,\beta}{K,\zeta}\right)$.

Obviously, for $n=2$ we obtain the algebra $\mathbb{H}_K\,(\alpha,\beta)$.

The quaternion generalized algebras and symbol algebras are central simple algebras.

Proposition 1.2. [8, pag. 237] *If K is an algebraic number field and A is a central simple $K-$algebra, then the dimension of A over K is a square.*

Definition 1.3. Let A be a central simple algebra of finite dimension n over K. The positive integer $d=\sqrt{n}$ is called *the degree* of the algebra A.

Theorem(**Weddeburn**).[8, pag. 50] *Let A be a central simple algebra over the field K. There are $n \in \mathbb{N}^*$ and a division algebra D, $K \subseteq D$, such that $A \simeq \mathcal{M}_n\,(D)$. The division algebra D is unique up to an isomorphism.*

Definition 1.4. With the notation of the above Theorem, the degree of the algebra D over K (as an algebra) is called *the index* of the algebra A.

For some $h \in N^*$, the tensor product over the field K $A \otimes ... \otimes A$ ($h-$ times) is isomorphic to a full matrix algebra over K.

Definition 1.5. The smallest such an h is called *the exponent* of the algebra A.

Theorem 1.6.[1] *The algebra A is a division algebra if and only if its index and its degree are the same.*

Theorem 1.7. (Brauer-Hasse-Noether).[8] *Every central simple algebra over an algebraic number field is cyclic and its index is equal to its exponent.* We shall use in the third section some results from the theory of algebraic number fields and we recall these here.

Theorem 1.8. ([1]) *Let $K \subseteq E$ be a cyclic extension of commutative fields of degree d. The cyclic $K-$algebra $A = \left(\frac{\alpha,\beta}{K,\zeta}\right)$ has the exponent d if and only if $\alpha \notin N_{L/K}(L^*)$, for each minimal subfield L of E over K.*

Theorem 1.9.([4]) *Let K be a field such that $\zeta \in K,\ \zeta^n = 1, \zeta$ is a primitive root, and let $\alpha, \beta \in K^*$. Then the following statements are equivalent:*

i) The cyclic algebra $A = \left(\frac{\alpha,\beta}{K,\zeta}\right)$ is split.

ii) The element β is a norm from the extension $K \subseteq K(\sqrt[n]{\alpha})$

Theorem 1.10. ([1;2;6]) *Let K be an algebraic number field, v be a prime of K and $K \subseteq L$ a Galois extension. Let w be a prime of L lying above v such that $K_v \subseteq L_w$ is a unramified extension of K_v of (residual) degree f. Let $b = \pi_v^m \cdot u_v \in K_v^*$, where π_v denote a prime element in K_v and u_v a unit in the ring of integers $\mathcal{O}_v, m \in \mathbb{Z}$. Then $b \in N_{L_w\,/\,K_v}(L_w^*)$ if and only if $f \mid m$. In particular, every unit of $\mathcal{O}_v$ is the norm of a unit in L_w.*

Theorem 1.11. ([2;7]) *Let K be an algebraic number field, e be an admissible modulus of K, v be a finite prime of K, v divides e. Let $K \subseteq L$ be a Galois extension. Let w be any prime of L lying above v. Then an element $a \in N_{L_w\,/\,K_v}(L_w^*)$ if and only if the Artin symbol $\left(\frac{L_w\,/\,K_v}{(a)}\right)$ is the identity in the Galois group $Gal(L_w\,/\,K_v)$, where (a) denotes the ideal generates by a in the ring of integers $\mathcal{O}_v$.*

Theorem 1.12. ([6]) *Let ζ be a primitive root of the unity of $l-$order, where l is a prime natural number and let A be the ring of integers of the Kummer field $Q(\zeta, \sqrt[l]{\mu})$. A prime ideal P in the ring $\mathbb{Z}[\zeta]$ is in A in one of the situations:*

i) It is equal with the $l-$power of a prime ideal from A, if the $l-$power character $\left(\frac{\mu}{P}\right)_l = 0$;

ii) It is a prime ideal in A, if $\left(\frac{\mu}{P}\right)_l =$ a rot of order l of unity, different from 1.

iii) It decomposes in l different prime ideals from A, if $\left(\frac{\mu}{P}\right)_l = 1$.

Theorem 1.13. ([5;6]) *Let l be a natural number, $l \geq 3$ and ζ be a primitive root of the unity of l-order. If p is a prime natural number, l is not divisible with p and f is the smallest positive integer such that $p^f \equiv 1$ mod l, then we have*

$$p\mathbb{Z}[\zeta] = P_1 P_2 .... P_r,$$

where $r = \dfrac{\varphi(l)}{f}$, φ is the Euler's function and $P_j,\ j = 1, ..., r$ are different prime ideals in the ring $\mathbb{Z}[\zeta]$.

In the following, we consider the symbol algebra for $n = 3$ and $K = \mathbb{Q}(\varepsilon)$ or $\mathbb{Q}_p(\varepsilon)$, where ε is a primitive cubic root of unity and p a prime number.

2. Some example of quaternion and symbol algebras

Proposition 2.1. *For $\alpha = -1, \beta = p, p = 4k+3$, a prime number, $K = \mathbb{Q}$, the algebra $\mathbb{H}_{\mathbb{Q}}(-1, p)$ is a division algebra.*

Proof. Let $x \in \mathbb{H}_{\mathbb{Q}}(-1, p)$, $x = x_0 \cdot 1 + x_1 e_2 + x_2 e_2 + x_3 e_3$, $x_i \in \mathbb{Q}$, $i = 0, 1, 2, 3$ such that $n(x) = 0$. It results $x_0^2 + x_1^2 - p x_2^2 - p x_3^2 = 0$, then $p \mid (x_0^2 + x_1^2)$. Since $p = 4k+3$ is a prime and $p \mid (x_0^2 + x_1^2)$, we obtain that $p \mid (x_2^2 + x_3^2)$, and the powers of p in the factorization of $x_0^2 + x_1^2$ and $x_2^2 + x_3^2$ are even. We obtain a contradiction, therefore $x = 0$.□

Theorem (Gauss). If $p \equiv 1$ *mod* 3, then there are integers a, b such that $4p = a^2 + 27b^2$.

Proposition 2.2. *If $K = \mathbb{Q}(\sqrt{3})$, then the quaternion algebra $\mathbb{H}_K(-1, p)$, where $p \equiv 1$ mod 3 is a split algebra.*

Proof. Indeed, $\mathbb{H}_K(-1, p)$ is a split algebra if and only if the associated conic $-x^2 + py^2 = z^2$ has $\mathbb{Q}(\sqrt{3}) -$ rational points. Using the Gauss's theorem, there are $a, b \in \mathbb{Z}$ such that $4p = a^2 + 27b^2$. Then for $y_0 = 1, z_0 = \frac{a}{2}$, $x_0 = \frac{3\sqrt{3}b}{2}$, the point $\left(\frac{3\sqrt{3}b}{2}, 1, \frac{a}{2}\right)$ is a $\mathbb{Q}(\sqrt{3}) -$ rational point for the associated conic, and we use Proposition 1.1.□

From the Wedderburn theorem, we know that a finite dimensional simple algebra A over a field K is isomorphic to a matrix algebra $\mathcal{M}_n(D)$, for D a division algebra. Let $K = \mathbb{Q}(\varepsilon)$ where ε is a cubic root of unity and let $d = [D : K]$ be the index of the algebra A. The algebra $A = \left(\frac{\alpha,\beta}{K,\zeta}\right)$ is a central simple algebra of degree 3, hence $d \mid 3$.

For $\alpha = -1, \beta = 1$, the algebra A is generated, for example, by the elements

$$X = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -\varepsilon & 0 \\ 0 & 0 & -\varepsilon^2 \end{pmatrix} \text{ and } Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

where $X^3 = -1 I_3$, $Y^3 = I_3$ and $YX = \varepsilon XY$. (see[3]) We obtain that $A \simeq \mathcal{M}_n(\mathbb{Q}(\varepsilon))$. Therefore $d = 1$ and the algebra A is not a division algebra.

We obtain the following proposition

Proposition 2.3. *The algebras $A = \left(\frac{\alpha,\beta}{\mathbb{Q}(\varepsilon),\varepsilon}\right)$, for $\alpha, \beta \in \{-1, 1\}$ are not division algebras.*

Proof. The algebra A has dimension 9, hence degree 3, with basis $B = \{1, x, y, x^2, y^2, xy^2, xy, x^2y, x^2y^2\}$, $x^3 = a, y^3 = b$. With the correspondence $x \to X, y \to Y$, we have that $A \simeq \mathcal{M}_n(\mathbb{Q}(\varepsilon))$, the index $d = 1 \neq 3$, where 3 is the algebra's degree, then A is not a division algebra.(We used Proposition 1.6.)□

If the central simple algebra A is a division algebra, since has the degree three, it results that it is a cyclic algebra. It results that there are the elements $x \in A-K$, $\alpha \in K$ such that $x^3 = \alpha \in K$. From the Noether-Skolem theorem, it results that there is an element $y \in A - K$ such that $yxy^{-1} = \varepsilon x$. We have $y^3x = xy^3$ and $y^3y = yy^3$, then y^3 commutes with the generators x, y, therefore $y^3 \in K = C(A)$, the centralizer of the algebra A. Hence, there is $\beta \in K$ such that $y^3 = \beta$, and $A = \left(\frac{\alpha,\beta}{K,\zeta}\right) \simeq \mathcal{M}_n(D)$, with $[D : K] = 3$.

3. The algebra $A = \left(\frac{\alpha,\beta}{K_v,\varepsilon}\right)$

We consider the case of the algebra $A = \left(\frac{\alpha,\beta}{K_v,\varepsilon}\right)$ where ε is a primitive cubic root of unity. We give a necessary and sufficient condition for a K_v-cyclic central simple algebra $A = \left(\frac{\alpha,\beta}{K_v,\varepsilon}\right)$ to be a division algebra and finally we find when β is a norm for the field $K_v\left(\sqrt[3]{\alpha}\right)$, where K_v is the completion of the field K with respect the v-adic valuation.

Let K be an algebraic number field and v be a prime (finite or infinite) of K such that $\varepsilon \in K_v$, where ε is a primitive cubic root. We consider the K_v- central simple algebra $A = \left(\dfrac{\alpha,\beta}{K_v,\varepsilon}\right)$, $\alpha,\beta \in K_v^*$.

Proposition 3.1. *With the above notation, if $L = K\left(\sqrt[3]{\alpha}\right)$, the following statement are equivalent:*

i) The algebra $A = \left(\dfrac{\alpha,\beta}{K_v,\varepsilon}\right)$ is a division algebra.

ii) $\beta \notin N_{L_w\,/\,K_v}\left(L_w^*\right)$, for each w a prime of L lying above v.

Proof. We consider the cyclic extension of fields $K_v \subseteq L_w$ and we apply the Theorems 1.6, 1.7, 1.8. We obtain that the K_v-cyclic central simple algebra $A = \left(\dfrac{\alpha,\beta}{K_v,\varepsilon}\right)$ is a division algebra if and only if $\beta \notin N_{L_w/K_v}\left(L_w^*\right)$.□

From the above proposition and the Theorem 1.9, result that a K_v-cyclic central simple algebra $A = \left(\dfrac{\alpha,\beta}{K_v,\varepsilon}\right)$ is either split or a division algebra.

In the following, we will study the central simple algebra $A = \left(\frac{\alpha,\ p^{3l}}{K_p, \varepsilon} \right)$, where p is a prime natural number, $p > 3, l \in \mathbb{N}^*$, ε is a primitive cubic root of unity, $K = \mathbb{Q}(\varepsilon)$.

Proposition 3.2. *Let p be a prime natural number, $p \equiv 2$ (mod 3) and let be given the K_p- algebra where $l \in \mathbb{N}^*, \alpha \in K, K = \mathbb{Q}(\varepsilon)$. Let P be a prime ideal of the ring of integers of the field $L = K(\sqrt[3]{\alpha})$, lying above p. Then p^{3l} is a norm from L_P^* and the local Artin symbol $\left(\frac{L_P \,/\, K_p}{(p^{3l})} \right)$ is the identity.*

Proof. Since $p \equiv 2 \pmod 3$, from Theorem 1.13., we obtain that p is prime in the ring $\mathbb{Z}[\varepsilon]$. It results that cubic residual symbol $\left(\frac{\alpha}{p_1\mathbb{Z}[\varepsilon]} \right)_3 = 1$, from Theorem 1.12, we have that p is totally split in $\mathbb{A}$, where $\mathbb{A}$ is the ring of integers of the field $L = K(\sqrt[3]{\alpha})$: $p\mathbb{A} = P_1P_2P_3,\ P_i \in Spec(\mathbb{A}), i = \overline{1,3}$.
We denote with g the number of decomposition of the ideal $p\mathbb{A}$ in the extension $K \subset L$. It results $g = 3$ and knowing that $efg = [L : K] = 3$, then $f = e = 1$. But $[L_P : K_p] = ef$, therefore $L_P = K_p$, for each $P \in Spec(\mathbb{A}), P \mid p\mathbb{A}$. In this case, we obtain that p is the norm of itself in the trivial extension of K_p and the Artin symbol $\left(\frac{L_P \,/\, K_p}{(p^{3l})} \right)$ is the identity.□

Proposition 3.3. *Let p be a prime natural number, $p \equiv 1$ (mod 3) and let $K_{p_1}-$ algebra $A = \left(\frac{\alpha, p^{3l}}{K_{p_1}, \varepsilon} \right)$, where $l \in \mathbb{N}^*, \alpha \in K, K = \mathbb{Q}(\varepsilon)$ and p_1 is a prime element in $\mathbb{Z}[\varepsilon]$, $p_1 \mid p$. Let P be a prime ideal in the ring of integers of the field $L = K(\sqrt[3]{\alpha})$, lying above p_1. Then $p^{3l} \in N_{L_P/K_{p_1}}(L_P^*)$ and the local Artin symbol $\left(\frac{L_P \,/\, K_{p_1}}{(p^{3l})} \right)$ is the identity in the Galois group $Gal(L_P/K_{p_1})$.*

Proof. From Theorem 1.13 and that $\mathbb{Z}[\varepsilon]$ is a principal ring, we have that the ideal $p\mathbb{Z}[\varepsilon] = p_1\mathbb{Z}[\varepsilon] \cdot p_2\mathbb{Z}[\varepsilon]$, where p_1, p_2 are prime distinct elements in $\mathbb{Z}[\varepsilon]$.

We study the $K_{p_1}-$ algebra $A=\left(\dfrac{\alpha,p^{3l}}{K_{p_1},\varepsilon}\right)$.

Case 1. If the cubic residual symbol $\left(\dfrac{\alpha}{p_1\mathbb{Z}[\varepsilon]}\right)_3$ is a root of unity different from 1, from Theorem 1.12, we obtain that the ideal $p_1\mathbb{A}\in Spec\left(\mathbb{A}\right)$,where $\mathbb{A}$ is the ring of integers of the Kummer field $K\left(\sqrt[3]{\alpha}\right)$. So that $e=1,g=1$ and since $efg=\left[K\left(\sqrt[3]{\alpha}\right):K\right]=3$, it results that $f=3$, who obviously divides $3l$. From Theorem 1.10, we obtain that $p^{3l}\in N_{L_P/K_{p_1}}\left(L_P^*\right)$. Using Theorem 1.11 and Proposition 3.1, we have that the local Artin symbol $\left(\dfrac{L_P\,/\,K_{p_1}}{(p^{3l})}\right)$ is the identity in the Galois group $Gal\left(L_P/K_{p_1}\right)$ and the algebra $A=\left(\dfrac{\alpha,p^{3l}}{K_{p_1},\varepsilon}\right)$ is not a division K_{p_1} algebra.

Case2. If the cubic residual symbol $\left(\dfrac{\alpha}{p_1\mathbb{Z}[\varepsilon]}\right)_3=1$, from Theorem 1.12, we obtain that $p_1\mathbb{A}=P_1P_2P_3,\ P_i\in Spec\left(\mathbb{A}\right),i=\overline{1,3}$, therefore $g=3$. But $efg=\left[K\left(\sqrt[3]{\alpha}\right):K\right]=3$, therefore $e=f=1$. Since $\left[L_P:K_{p_1}\right]=ef$, we obtain that $L_P=K_{p_1}$ for each $P\in Spec\left(\mathbb{A}\right),p\mid p_1\mathbb{A}$. In this case, we have that p_1 is a norm of itself in the trivial extension of K_{p_1} and the local Artin symbol $\left(\dfrac{L_P\,/\,K_{p_1}}{(p^{3l})}\right)$ is the identity.□

Acknowledgements
The first author is indebted to Senior Research Fellow Tamas Szamuely, from Alfréd Rényi Institute of Mathematics from Budapest for the many helpful discussions.

References

[1] Acciaro, V., *Solvability of Norm Equations over Cyclic Number Fields of Prime Degree*, Mathematics of Computation, **65**(216)(1996), 1663-1674.

[2] Acciaro,V., Kluners, J., *Computing Local Artin Maps, and Solvability of Norm Equations*, Journal Symbolic Computation **11**(2000), 1-14.

[3] Elduque, E., *Okubo algebras and twisted polynomials*, Contemporary Mathematics, **224**(1999), 101-109.

[4] Gille, P., Szamuely, T., *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, 2006.

[5] Ireland,K., Rosen M. *A Classical Introduction to Modern Number Theory*, Springer Verlag, 1992.

[6] Janusz, G.J., *Algebraic number fields*, Academic Press, London, 1973.

[7] Milne, J.S., *Class Field Theory*, http://www.math.lsa.umich.edu/ jmilne.

[8] Pierce, R.S., *Associative Algebras*, Springer Verlag, 1982.

[9] Schafer, R. D., *An Introduction to Nonassociative Algebras*, Academic Press, New-York, 1966.

UNIVERSITY "OVIDIUS"
DEPARTMENT OF MATHEMATICS AND INFORMATICS
BD. MAMAIA 124, 900527, CONSTANTA, ROMANIA
E-mail address: savin.diana@univ-ovidius.ro, cflaut@univ-ovidius.ro, cristina_flaut@yahoo.com

DEPARTMENT OF MATHEMATICS-INFORMATICS AND FUNDAMENTAL TECHNICAL SCIENCES
MIRCEA CEL BATRAN NAVAL ACADEMY
1, FULGERULUI SREET, 900218, CONSTANTA, ROMANIA
E-mail address: c_cami_ro@yahoo.com